



الفيروسات وطرق الحماية منـها

إعــــداد

أشـرف حســين الأشـقـر

ما هو فيروس الحاسوب

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن فيروسات الكوبأنه: هي برامج تتم كتابتها بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه، وتتم كتابتها بطريقة معينة .

تتصف فيروسات الحاسب بالتالي :

1- برنامج قادر على التناسخ Replication والانتشار .
2- فيووس يربط نفسه ببرنامج أخر يسمى الحاضن
3- لا يمكن أن تنشأ الفيروسات من ذاتها.
4- يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي:

1- آلية التناسخ : وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

2-آلية التخفي : وهو الجزء الذي يخفي الفيروس عن الاكتشاف.

3-آلية التنشيط : وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يتم تشغيله ، كاستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام.

4- آلية التنفيذ : وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه.طرق انتقال الفيروسات

طريقة العدوى بالفيروسات :

يمكن أن نميز فئتين من فيروسات الحاسوب تبعاً لآلية العدوى وانتشار الفيروس:

1- فيروس العدوى المباشر (Direct Infector) :

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع، فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه، وعندما يصاب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله ،وهذا النوع قليل الانتشار.

2- فيروس العدوى غير المباشر (Indirect Infector) :

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع، فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها، ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله إلى الذاكرة بعد ذلك، إلى أن يتم قطع التغذية الكهربائية عن الحاسوب أو إعادة تشغيله.

أسباب التسمية باسم (Virus) :

سمي الفيروس (Virus) بهذا الاسم لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

أولا : الفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا
ثانيا : تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة (RAM) مثلا وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة كلما طال وقت اكتشاف الفيروس تستخدم عادة لغة التجميع (الاسمبلي) لكتابة كود تنفيذ الفيروس

أنواع الملفات التي يمكن أن يصيبها الفيروس:

الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (EXE , COM)ضمن أنظمة التشغيل دوس وميكروسوفت ويندوز أو (ELF) في أنظمة لينكس

سجلات الملفات والبيانات (VOLUME BOOT RECORD)في الأقراص المرنة والصلبة .

(MASTER BOOT)ملفات الأغراض العامة مثل ملفات الباتش والسكريبتات في ويندوز وملفات الاستخدام المكتبي في النوافذ (WINDOWS)التي تحتوي علي مثل الورد والإكسل وأكسس .

قواعد البيانات وملفات الاوتلوك لها دور كبير في الإصابة ونشر الإصابة لغيرها لما تحويه من عناوين البريد الالكتروني

ملفات الاكروبات (PDF) وبعض النصوص المهجنة (HTML) احتمال احتوائها على كود خبيث .

أعراض الإصابة بالفيروس :

١ -ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
٢ -تكرار اختفاء بعض الملفات التنفيذية.
٣ -حدوث بطء شديد في إقلاع[نظام التشغيل] أو تنفيذ بعض التطبيقات ورفض بعض التطبيقات للتنفيذ.
٤ -عند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في قرص صلب أو المرن، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر وبطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أوالإنترنت أو تبادل الأقراص المرنة.

تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجه هناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على إشغال المعالج بحيث تبطئ سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل أرقام حسابات وكلمات السر أو أرقام بطاقات الائتمان وبيانات مهمة أخرى وهذه أهم أهداف

الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم .

أنواع الفيروسات الشهيرة

وتنقسم إلى أربعة أنواع هي :

١ -الفيروس 2- الدودة 3- حصان طروادة 4- فيروس (Brontok)

ما الفرق بين الفيروس والدودة وحصان طروادة ؟

1-الفيروس :يمكن القول بأنه برنامج تنفيذي (ذات نوع scr, pif, bat, exe com) ويعمل بشكل منفصل ويهدف إلى أحداث خلل في نظام الحاسوب وتتراوح خطورته حسب مهمته فمنه الخطير ومنه الخفيف وكلاهما خبيث.وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز أخر عن طريق الأقراص المدمجة سي دي وذاكرة الفلاش.

2-الدودة :(**worm**) تنتشر فقط عبر الشبكات والانترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الالكتروني مثلا فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا... مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم اعتبره فيروس ومنهم من اعتبره برنامج خبيث وذلك كون الدودة لا تنفذ أي عمل مؤذي إنما تنتشر فقط مما يؤدي إلى إشغال موارد الشبكة بشكل كبير ومع التطور الحاصل في ميدان الحوسبة أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها مثلا (في يوم معين أو ساعة أو تاريخ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة تسمى (هجمات حجب الخدمة) حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهميه لجاهز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة) فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا مما يسبب

توقفه عن العمل وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت وغيرها الكثير.

3-حصان طروادة :Trojan Horse سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما
ومثال ذلك تم توزيع قرص مجاني على المستشفيات به برنامج حول مرض الايدز (أسبابه - طرق انتشاره - طرق العلاج.. الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسب الحاضنة للفيروس وظهرت رسالة مفادها أن الحاسب مصاب بالايدز (المقصود هنا انه تم تشفير ملفات الحاسب وإيقافها عن العمل بطريقه نظاميه) أرسل مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشيفره مما اجبر المختصين بالرضوخ للطلب كونهم لم يقدروا على فك التشفير.
توجد عدة تقسيمات للفيروسات، فمثلاً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات.

أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة طبعا لا يوجد فيروسات خارقه بحيث إنها تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسبب الفيروس تعطلت وحدة التغذية بسبب الفيروس أو تلفت الشاشة بسبب الفيروس... الخ) ولكن يمكن للفيروس أن يؤذي الذاكرة روم في الحاسب كما في فيروس تشرنوبل أو أن يمحي معلومات الـ(Main Boot Sector) على القرص الصلب فتعود الأقراص الصلبة كما أتت من المصنع وفي الحالتين السابقتين لا يتم إقلاع الجهاز مما يوحي للبعض أن الفيروس (حرق) الحاسب طبعا هذه الفيروسات تعتبر خطيرة جدا لأنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمة، وهنالك أيضا الفيروسات المدمرة للبرامج وتأثيرها محدود طالما أن البيانات لم تتأثر حيث يمكن تخزين البيانات وإعادة تهيئة الحاسب

وإعادة البرامج المتضررة من أقراصها الأصلية ، والفيروسات عديمة الضرر وهي التي لا تقوم بأي عمل مؤذي وإنما تم برمجتها لإثبات الذات والقدرة على البرمجة من بعض المراهقين فمنها ما يرسم كرة أو أي شكل على الشاشة طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الأحرف (كتغير حرف بحرف أينما وجد) أو تغيير مؤشر الماس.. الخ.

4- فيروس Brontok : (الفيروس الذي يخفي خيارات المجلد أو يفقدك التحكم في الرجستري فتصبح غير قادر على التحكم في الحاسوب) وهذا الفيروس من أبرز مهامه أنه يقوم بإخفاء خيارات المجلد من قائمة أدوات الموجودة في نظام الويندوز وأيضا يقوم بتكرار جميع المجلدات التي يصيبها حتى أنك لاتعرف الأصل من النسخة وقد تحذف الأصل ظنا منك أنه الفيروس، وهو أيضا يقوم بفتح شاشة الإنترنت إكسبلورر ويقوم بفتح شاشة خضراء اللون بشكل مستمر مما يسبب بطء في النظام وما يؤدي إلى زيادة انتشار هذا الفيروس في الكمبيوتر

فيروس xcopy والذي يصيب الـ Partion القسم للقرص الصلب ويجعله لا يفتح مباشرة وذلك بزرع ملف auotorun وحينما تحاول فتح القسم يعطيك قائمة فتح باستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل)استكشاف وتشغيل) للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يصيح باستمرار مطالبا بإدخال قرص مرن للكمبيوتر .

تصنيف الفيروسات حسب خطورتها:

1- **العادي (Trivial)**: لا يفعل الفيروس العادي شيئا سوى التكاثر replication ولا يسبب أي ضرر أو تخريب للمعلومات مثل فيروس stupid .

2- **الثانوي (Minor):** يصيب الملفات التنفيذية فقط executable file ولا يؤثر على البيانات .

3- **المعتدل (Moderate) :** يقوم بتدمير جميع الملفات الموجودة على القرص إما باستبدال المعلومات بمعلومات لا معنى لها أو عن طريق إعادة التهيئة Reformatting مثل فيروس Disk killer الذي يقوم بإعادة تهيئة القرص. ويمكن

حل مشكلة هذه الفيروسات عن طريق استخدام النسخ الاحتياطي .

4- الرئيسي (Major):يؤدي الفيروس إلى تخريب المعلومات بإجراء تغيرات ذكية وبارعة للبيانات دون أن يترك أثرا يشير إلى التغيير الحاصل كأن يقوم بتبديل كتل المعلومات المتساوية في الطول بين الملفات كما أن تأثيره يكون على المدى الطويل ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام وبذالك لا يمكن الوثوق بالنسخة الاحتياطية أيضا.

5- اللامحدود (Unlimited): يستهدف الشبكات والملفات المشتركة وتمضي أكثر الوقت في محاولة معرفة كلمة السر للمستخدمين الأكثر فاعلية وعند معرفتها يقوم بتمريرها إلى أحد أو أكثر من مستخدمي الشبكة على أمل أنهم سيستخدمونها لأغراض سيئة.

لقد أصبحنا نعرف أننا معرضين للهجوم من قبل الفيروسات ولكن بالمقابل نرى مدى التعقيد والترابط الذي وصل إليه الإنسان فعلى سبيل المثال:

- فيروس (My doom) قدر الخبراء الحواسيب المتضررة من هذه الدودة بحوالي ربع مليون حاسوب خلال يوم واحد والذي كان في كانون الثاني2004.

- فيروس (Melissa) أعطى هذا الفيروس فاعلية كبيرة جدا حيث أجبر شركة Microsoft والعديد من كبرى الشركات الأخرى على إطفاء مخدمات البريد بشكل كامل حتى تمكنوا من القضاء عليه وذلك في آذار 1999 وفي الشهر الأول من عام 2007 ظهرت دودة اسمها Storm وبحلول الشهر التاسع كان أكثر من 50 مليون حاسوب مصاب .كلنا تصور أن كل هذا التأثير ينتج عن برامج بسيطة جدا.

ومن أخطار فيروس Melissa أنه يقوم بإنشاء الفيروس على شكل مستند Word ووضع في موقع للأخبار عندما يقوم أي شخص بتحميل الملف وفتحه فإن الفيروس يتفعل ويقوم بإرسال المستند إلى أول 50 شخص في الـAddress book والمستند يحوي على ملاحظة لطيفة واسم الشخص المرسل إليه وعندما يقوم المرسل إليه بفتح المستند يتم إرساله إلى 50 شخص أخر وبهذه الطريقة أصبح فيروس Melissa أسرع فيروس في الانتشار

استخدم الفيروس I love you الطريق نفسها لكن عوضا عن نسخ نفسه تلقائيا فأنه

كان يربط كوده برابط معين ضمن الرسالة وعند النقر عليه كان يرسل نفسه إلى جميع العناوين الموجودة في (Address book) استخدم الفيروس ميزة الموجودة في VBA (visua basic for application) وهي لغة برمجة كاملة وتستطيع من خلالها أن تبرمج أي شيء مثل تعديل ملف أو إرسال الرسائل الالكترونية أي يمكنك كتابة أي برنامج وعند فتح المستند يتم تنفيذه طبعا هي ميزة مفيدة ولكنها في نفس الوقت ميزة تنفيذ تلقائية .

لماذا يقوم المبرمجين بعمل فيروسات الحاسوب

فيروسات الحاسوب لا تتشابه في وجودها بالفيروسات الحيوية. إن فيروس الحاسوب لا ينشأ من لا شيء ولا يأتي من مصدر مجهول ولا ينشأ بسبب خلل بسيط حدث في الحاسوب. فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمه بشكل متقن. يعمل المبرمجون على برمجة الفيروسات وذلك لأهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لأنة بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون للشراء .يذكر أن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر .أما الأهداف العسكرية فهي محاولة الدخول لأنظمة الطرف الأخر لكشف أسرار واخذ بيانات عن طريق برامج التجسس. الأهداف الإجرامية فأهمها سرقة بيانات وأرقام حسابات أو أرقام بطاقات الائتمان وكلمات السر لمحاولة الدخول لحسابات المشتركين في البنوك وسرقة أموالهم. أو سرقة بيانات من اجهزتهم لأبتزازهم

الخطوات الأساسية لحماية جهازك وبياناتك الشخصية

في ظل الإقبال الشديد على استخدام الحاسب الآلي والاتصال بشبكة الإنترنت لإنجاز العديد من المهام اليومية سواءً المتعلقة بطبيعة الوظيفة أو الدراسة أو الترفيه أو الأعمال الحرة، أصبح من المؤرق ومن الصعب على المستخدم العادي الحفاظ على أمن وخصوصية معلوماته وحماية جهازه الشخصي من المخاطر المحيطة به مثل الفيروسات أو المخترقين بشكل خاص.

كلنا يستعمل أثناء عمله في الحاسوب عملية النسخ واللصق سواء في المعلومات التبادلية أو في الأشياء الشخصية في تصفح الإنترنت وعند استخدامك اختصارات الكيبورد لاسيما منها النسخ Ctrl+cو اللصق Ctrl+v فإنه وللأسف بتركيبة من لغات البرمجة الحديثة مدعمة بـ ASP تستطيع بعض المواقع تسجيل ما قمت من نسخة على الشاشة سواء كان نصاً أو كلمة مرور أو رقما لبطاقة بنكية أو غير ذلك من المعلومات لذا وجدت أنه من المفيد أن ألخص أهم الخطوات الأساسية والبسيطة والتي من خلالها يستطيع المستخدم أن يحد بشكل كبير من تلك المخاطر التي قد يتعرض لها أثناء استخدامه لشبكة الإنترنت .وتتكون هذه الخطوات من عشرة نصائح توفر إلى درجة كبيرة مستوى مقبول من الأمان

والمحافظة على الخصوصية وهي كالتالي :

1- تحديث نظام التشغيل والبرامج المستخدمة وتفعيل خاصية التحديث التلقائي. من المهم جداً أن يقوم المستخدم بتحديث نظام التشغيل الخاص بجهازه (مثل نظام التشغيل (Windows بشكل دوري وذلك بتحميل آخر الإصدارات والتحديثات الخاصة بالثغرات الأمنية والتشغيلية للنظام وذلك إما بزيارة موقع الشركة المطورة وتحميل تلك التحديثات بشكل دوري أو بتفعيل خاصية التحديث التلقائي والمتوفرة في نظام التشغيل. وتعتبر الطريقة الأخيرة هي الأسلم والأسهل كونها لا تتطلب من المستخدم المتابعة المستمرة لآخر التحديثات. وينطبق نفس المبدأ على أي برامج أخرى موجودة في الجهاز مثل برامج Microsoft Office أو Adobe Acrobatأو Java أو غيرها من برامج الصوتيات والمحادثة وبرامج ضغط الملفات. وتكمن أهمية هذه التحديثات بضمان استمرار فعالية وأمان تلك البرامج والتي غالباً ما يكون الإصدار

الأولي والمبدئي منها مليء بالثغرات والعيوب الأمنية أو التشغيلية والتي من الممكن أن تستغل من قبل المخترقين بشكل سلبي. لذلك تقوم الشركات المطورة لتلك البرامج بمعالجة تلك العيوب بإصدار نسخ جديدة أو تحديثات لبرامجهم بشكل دوري .

2- استخدام برنامج مضاد للفيروسات وتفعيل خاصية التحديث التلقائي. تقوم البرامج المضادة للفيروسات بالكشف عن أي برامج أو ملفات مشبوهة قد تشكل خطراً على جهاز المستخدم أو بياناته ومحاولة إزالة تلك البرامج الضارة أو تعطيل عملها وعزلها. ومن الضرورة القصوى أن يكون برنامج مضاد الفيروسات محتوياً على آخر التحديثات الخاصة بالفيروسات الجديدة والتي انتشرت مؤخراً. إذ أن مجرد وجود برنامج مضاد للفيروسات غير محدث غير كافٍ لحماية الجهاز بشكل فعال. فهناك ما يقارب مئات الفيروسات الجديدة التي تصدر بشكل يومي. ولكي تسهل عملية التحديث على المستخدم، ينصح بتفعيل خاصية التحديث التلقائي والتي توفرها جميع برامج مضادات الفيروسات .

3- استخدام برنامج الجدار الناري للحماية من المتطفلين والمخترقين. من البرامج الهامة أيضاً في عملية حماية الجهاز هو برنامج الجدار الناري (Firewall) والذي يعمل بشكل أساسي كمصفاة (أو فلتر) لمنع جميع طلبات الاتصال الغير مصرح لها والقادمة من شبكة الإنترنت على وجه الخصوص، وهو ما يوفر الحماية للمستخدم بصد أي محاولة قد يقوم بها المخترق للاتصال بجهاز المستخدم عن بعد. والجدير بالذكر أن أغلب الإصدارات الحديثة لأنظمة التشغيل تقدم هذا البرنامج بشكل مجاني مما يوفر على المستخدم تكلفة شرا برنامج خاص لهذا الغرض .

4- استخدام برنامج مضاد للبرامج الدعائية والتجسسية وتفعيل خاصية التحديث التلقائي. من المزعج جداً ما تقوم به بعض البرامج التجارية الدعائية(Adware/Spyware) من فتح نوافذ وصفحات إعلانية عن منتج معين أو موقع معين وذلك أثناء تشغيل الجهاز أو أثناء تصفح شبكة الإنترنت. وتتمثل خطورة هذا النوع من البرامج أيضاً بما تقوم به من جمع معلومات شخصية عن المستخدم مثل البريد الإلكتروني أو المواقع التي تمت زيارتها أو غيرها من المعلومات الخاصة. ولحسن الحظ تتوفر العديد من البرامج المضادة لتلك البرامج الدعائية والتي من السهل الحصول عليها من خلال شبكة الإنترنت بشكل مجاني

5- عدم تحميل وتشغيل أي برامج مجهولة المصدر. مما يساعد انتشار وتفشي أغلب الفيروسات وبرامج التجسس وبرامج الاختراق هو جهل المستخدم بالطريقة السليمة والآمنة لتحميل البرامج التي يرغب بها. إذ أن الطريقة المثلى لتحميل أي برنامج مرغوب به يفترض أن تتم بزيارة موقع الشركة الأم المطورة لذلك البرنامج وتحميله بشكل مباشر بدلاً من الاعتماد على المصادر الأخرى كالمنتديات أو مواقع الإنترنت الغير موثوقة أو من خلال برامج المحادثة أو البريد الإلكتروني. تشير الدراسات إلى أن أسرع وأسهل طريقة لانتشار الفيروسات وبرامج التجسس هي من خلال البريد الإلكتروني وذلك بمحاولة خداع وإيهام المستخدم بأن مرفقات البريد الإلكتروني سليمة وذات غرض مفيد أو ترفيهي. لذلك ينبغي توخي الحذر عند فتح أي من البرامج أو الملفات المرفقة التي لا يعرف مصدرها أو مرسلها أو سبب إرسالها. في حال استلام بريد إلكتروني مجهول المصدر ويحتوي على مرفقات ينصح بحذفه فوراً. أما في حال استلام بريد إلكتروني ويحتوي على مرفقات غير متوقعة أو مريبة من شخص معروف من قبل المستخدم فإنه من الأفضل الاتصال بالمرسل والتأكد من طبيعة تلك المرفقات قبل فتحها وتشغيلها .

6- عدم الاستجابة لأي بريد إلكتروني مشبوه يطلب معلومات شخصية. يتفنن محتالو شبكة الإنترنت بمحاولة خداع المستخدم العادي بطرق متنوعة ومتجددة رغبة منهم في الحصول على معلومات ثمينة تمكنهم من تنفيذ أهدافهم التخريبية أو الاحتيالية كسرقة الأموال من الحسابات البنكية أو من البطاقات الائتمانية أو ابتزاز المستخدم ومساومته على بياناته ووثائقه الخاصة. لذلك ينبغي على المستخدم ألا يستجيب لأي بريد إلكتروني يطلب منه معلومات شخصية كالاسم أو تاريخ الميلاد أو العنوان أو رقم الحساب البنكي أو رقم البطاقة الائتمانية. وتجدر الإشارة أيضاً إلى أن هناك أنواع أخرى من رسائل البريد الإلكتروني الاحتيالية (Phishing) والتي توهم المستخدم أنها مرسلة من قبل جهات موثوقة ومعروفة كالبنوك المحلية التي يتعامل معها المستخدم أو الشركات التجارية المعروفة، وتحتوي هذه الرسائل الإلكترونية على روابط مزيفة تبدو من الوهلة الأولى أنها روابط حقيقية وسليمة ولكنها في الواقع تقود المستخدم إلى مواقع مزيفة أيضاً تشابه إلى حد كبير تلك المواقع الحقيقية والأصلية التي يتعامل ويثق فيها المستخدم مما يجعله يقوم بإدخال معلوماته الشخصية كاسم المستخدم وكلمة المرور والذي من شأنه أن يمكن الشخص المحتال من الاستيلاء على حسابات ومعلومات المستخدم .

7- عدم استخدام أجهزة الحاسب الآلي العامة بإدخال معلومات حساسة وسرية. ينبغي أخذ الحيطة والحذر عند استخدام الأجهزة في الأماكن العامة كمقاهي الإنترنت أو المكتبات العامة أو المعامل وذلك بعدم إدخال أي معلومات حساسة وسرية مثل اسم المستخدم وكلمة المرور للبريد الإلكتروني أو معلومات الحساب البنكي أو غيرها من المعلومات الشخصية. وتكمن أهمية هذه النصيحة الاحترازية بطبيعة إدارة واستخدام تلك الأجهزة العامة سواءً من قبل مشرفيها الذين من الممكن أن يسيئوا استخدام صلاحياتهم أو من قبل مستخدمين آخرين لتلك الأجهزة وذلك باحتمال قيامهم بتسجيل جميع المعلومات التي يقوم المستخدم بإدخالها أثناء تصفحه لشبكة الإنترنت عبر برامج تجسسية خاصة لهذا الغرض.

8- استخدام كلمة مرور قوية ومعقدة وتغييرها بشكل دوري. قد يكون من السهل على المخترقين الدخول على حسابات المستخدم كالبريد الإلكتروني أو الحساب البنكي أو الجهاز الشخصي وذلك بتخمين كلمة المرور خصوصاً إذا كانت من الكلمات الدارجة أو الموجودة في القاموس أو التي ترتبط ببيانات المستخدم كتاريخ الميلاد أو رقم الهاتف أو رقم لوحة السيارة أو غيرها من البيانات التي قد يتمكن المخترق من تخمينها أو كسرها، علماً بأن هناك العديد من البرامج المتوفرة على شبكة الإنترنت والتي تساعد المخترق بتجريب آلاف الكلمات الشائعة أو الكلمات الموجودة في قواميس اللغة. لذلك، ينصح باختيار كلمة مرور معقدة تتكون من مختلف الحروف والأرقام والرموز بطول لا يقل عن ثمانية خانات لحمايتها من التخمين أو الكسر (Brute forcing)، وكذلك القيام بتغييرها بشكل دوري لضمان سريتها .

9- الحد والتقليل من استخدام برامج المشاركة الثنائية. توفر برامج المشاركة الثنائية (Peer-to-Peer) مثل BitTorrent أو Limewire أو Kazaa وسيلة سهلة وجذابة للعديد من مستخدمي الإنترنت بتداول ومشاركة الملفات الصوتية أو المرئية أو غيرها، وخصوصاً تلك الملفات المحفوظة قانونياً بحقوق الطبع والملكية الفكرية. ونظراً لسهولة انتقال الفيروسات وبرامج التجسس من خلال تلك البرامج، لابد من أخذ الحيطة والحذر عند تحميل أي ملفات عن طريق تلك البرامج والحد من استخدامها قدر الإمكان. أضف إلى ذلك إلى أنه من المخالف قانونياً تحميل أو مشاركة أي ملفات محفوظة فكرياً في الدول التي تطبق قوانين حماية الملكية الفكرية كالولايات المتحدة الأمريكية ودول أوروبا وغيرها من البلدان .

10- القيام بعمل نسخة احتياطية للبيانات والمعلومات الهامة. يعد عمل نسخة احتياطية (Backup)للملفات الهامة في الجهاز واحد من أهم الإجراءات الاحترازية التي ينبغي على المستخدم القيام بها بشكل دوري تحسباً لأي طارئ قد يحدث لتلك الملفات سواءً كان لعوامل فنية مثل فشل القرص الصلب أو لعوامل تخريبية كمسح ملفات المستخدم من قبل المخترق أو لعوامل أخرى كسرقة الجهاز أو ضياعه. ويمكن القيام بهذه الخطوة بشكل آمن وفعّال باستخدام وسائط تخزين مختلفة مثل الأقراص المدمجة (CDs) أو القرص الصلب الخارجي (External Hard Disk)أو الذاكرة اليدوية المتنقلة.(USB)

11- تثبيت برامج حماية من الباتشات اوافضلهم (The Cleaner) الابتعاد عن استخدام سكريبتات البرامج (Scripts) لأنها في الغالب تكون هناك فيروسات و باتشات مصاحبة لها .. ومسح جميع الكوكيز الموجودة على الجهاز وذلك بإتباع الطريقة التالية لتسريع جهازك وحمايته من الملفات الضارة :

من قائمة ابدأ (START) اختار الأمر تشغيل (RUN) ثم ضع كل أمر من الأوامر التي في الأسفل في المربع وأضغط موافق (OK) ثم ألغي كل الملفات التي سوف تعرض أمامك وطبق هذه الخطوة أربع مرات على حسب عدد الأوامر والأوامر هي :

(Recent ، Prefetch ، Temp ، %temp%)